日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　９月　１日

出願番号
Application Number: 平成１１年特許願第２４７０６０号

出願人
Applicant (s): 日本電信電話株式会社

２０００年　６月２３日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０４６８３６

【書類名】　特許願
【整理番号】　NTTH115900
【提出日】　平成11年 9月 1日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　鈴木　幸太郎
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100066153
　【弁理士】
　【氏名又は名称】　草野　卓
【選任した代理人】
　【識別番号】　100100642
　【弁理士】
　【氏名又は名称】　稲垣　稔
【手数料の表示】
　【予納台帳番号】　002897
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9806848
【プルーフの要否】　要

【書類名】明細書

【発明の名称】電子入札方法及び電子入札方法を記録した記録媒体並びに電子入札装置

【特許請求の範囲】

【請求項1】開札側の開札者Ａに対する入札側の複数の入札者$B_{i(i=1,2,\cdots,n)}$による入札に際して、開札側に備えた開札装置と入札側に備えた入札装置とをネットワークを介して接続し、入札を行なう電子入札方法において、

開札者Ａは入札価格表$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$および一方向性関数Ｈを決めて公開する手順１と、

入札装置は入札者B_iの入札価格ω_{vi}に対して入札値$b_{i,1}=b_{i,2}=\cdots=b_{i,vi-1}$=no（落札しない）、$b_{i,vi}$=yes（落札する）を計算する手順２と、

入札値に対して一方向性関数Ｈの連鎖によるコミットメント$L_{i,j}=H(b_{i,j},L_{i,j+1})$を計算し、コミットメント$L_{i,1}$とその署名$\sigma_i$の組$(L_{i,1},\sigma_i)$を入札として開札装置に送信する手順３と、

開札装置は送信されてきた入札$(L_{i,1},\sigma_i)$を受信する手順４と、

全入札者の入札装置からの入札が揃ったら署名σ_iが正当であることを検証し、全入札者の入札装置からの入札を公開する手順５と、

j=1とする手順６と、

入札装置からの入札値$(b_{i,j},L_{i,j+1})$を受信し、全入札者の入札値が揃ったらコミットメント$L_{i,j}$の正当性$L_{i,j}=H(b_{i,j},L_{i,j+1})$を検証し、全入札値｛$(b_{i,j},L_{i,j+1})$｝を公開する手順７と、

全てのiに対して入札値$b_{i,j}$=noならj=j+1として手順７へ戻る手順８と、

あるiに対して入札値$b_{i,j}$=yesならB_iを落札者、ω_jを落札価格として決定すると共に公開する手順９とを備えた

改竄などの不正がなく落札者および落札価格が正当であることを全入札者が検証可能であり、落札者以外の入札価格を秘匿し、一方向性関数の連鎖によるコミットメントを用いることにより効率的に入札が実現できること

を特徴とする電子入札方法。

【請求項２】開札側の開札者Ａに対する入札側の複数の入札者$B_{i(i=1,2,\cdots,n)}$

による入札に際して、開札側に備えた開札装置と入札側に備えた入札装置とをネットワークを介して接続し、入札を行なう電子入札方法において、

開札者Ａは入札価格表$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$および一方向性関数Ｈを決めて公開する手順１と、

入札装置は入札者B_iの入札価格ω_{vi}に対して入札値$b_{i,1}=b_{i,2}=\cdots=b_{i,vi-1}$=no（落札しない）、$b_{i,vi}$=yes（落札する）を計算する手順２と、

入札値に対して一方向性関数Ｈの連鎖によるコミットメント$L_{i,j}=H(b_{i,j},L_{i,j+1})$を計算し、コミットメント$L_{i,1}$とその署名$\sigma_i$の組$(L_{i,1},\sigma_i)$を入札として開札装置に送信する手順３と、

開札装置は送信されてきた入札$(L_{i,1},\sigma_i)$を受信する手順４と、

全入札者の入札装置からの入札が揃ったら署名σ_iが正当であることを検証し、全入札者の入札装置からの入札を公開する手順５と、

j=1とする手順６と、

入札装置からの入札値$(b_{i,j},L_{i,j+1})$を受信し、全入札者の入札値が揃ったらコミットメント$L_{i,j}$の正当性$L_{i,j}=H(b_{i,j},L_{i,j+1})$を検証し、全入札値｛$(b_{i,j},L_{i,j+1})$｝を公開する手順７と、

全てのiに対して入札値$b_{i,j}$=noならj=j+1として手順７へ戻る手順８と、

あるiに対して入札値$b_{i,j}$=yesならB_iを落札者、ω_jを落札価格として決定すると共に公開する手順９とを備えた

改竄などの不正がなく落札者および落札価格が正当であることを全入札者が検証可能であり、落札者以外の入札価格を秘匿し、一方向性関数の連鎖によるコミットメントを用いることにより効率的に入札を実現できること

を特徴とする電子入札方法を記録した記録媒体。

【請求項３】入札装置は入札者$B_{i(i=1,2,\cdots,n)}$が入札価格表$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$から選択した入札価格$\omega_{vi}$に対して入札値$b_{i,1}=b_{i,2}=\cdots=b_{i,vi-1}$=no（落札しない）、$b_{i,vi}$=yes（落札する）を計算する手順１と、

入札値$b_{i,j}$に対して一方向性関数Ｈの連鎖によるコミットメント$L_{i,j}=H(b_{i,j},L_{i,j+1})$を計算し、入札値$(b_{i,j},L_{i,j+1})$を開札装置に送信する手順２と、

コミットメント$L_{i,1}$とその署名σ_iの組$(L_{i,1},\sigma_i)$を入札として開札装置に

送信する手順３とを備えたこと

を特徴とする入札方法。

【請求項４】入札装置は入札者$B_{i(i=1,2,\cdots,n)}$が入札価格表$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$から選択した入札価格$\omega_{vi}$に対して入札値$b_{i,1}=b_{i,2}=\cdots=b_{i,vi-1}$=no（落札しない）、$b_{i,vi}$=yes（落札する）を計算する手順１と、

入札値$b_{i,j}$に対して一方向性関数Ｈの連鎖によるコミットメント$L_{i,j}=H(b_{i,j},L_{i,j+1})$を計算し、入札値$(b_{i,j},L_{i,j+1})$を開札装置に送信する手順２と、

コミットメント$L_{i,1}$とその署名σ_iの組$(L_{i,1},\sigma_i)$を入札として開札装置に送信する手順３とを備えたこと

を特徴とする入札方法を記録した記録媒体。

【請求項５】開札装置は入札者$B_{i(i=1,2,\cdots,n)}$から送信された入札$(L_{i,1},\sigma_i)$〔ただし、入札値$b_{i,1}$は入札価格表を$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$とした場合の$\omega_1$に対する入札値（yes：落札する、no：落札しない）、$L_{i,1}=H(b_{i,1},L_{i,2})$は入札値$b_{i,1}$のコミットメント、$\sigma_i$はコミットメント$L_{i,1}$の署名〕を受信する手順１と、

全入札者の入札装置からの入札が揃ったら署名σ_iが正当であることを検証し、全入札者の入札装置からの入札を公開する手順２と、

j=1とする手順３と、

入札装置からの入札値$(b_{i,j},L_{i,j+1})$を受信し、全入札者の入札値が揃ったらコミットメント$L_{i,j}$の正当性$L_{i,j}=H(b_{i,j},L_{i,j+1})$を検証し、全入札値$\{(b_{i,j},L_{i,j+1})\}$を公開する手順４と、

全てのiに対して入札値$b_{i,j}$=noならj=j+1として手順４へ戻る手順５と、

あるiに対して入札値$b_{i,j}$=yesならB_iを落札者、ω_jを落札価格として決定すると共に公開する手順６とを備えたこと

を特徴とする開札方法。

【請求項６】開札装置は入札者$B_{i(i=1,2,\cdots,n)}$から送信された入札$(L_{i,1},\sigma_i)$〔ただし、入札値$b_{i,1}$は入札価格表を$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$とした場合の$\omega_1$に対する入札値（yes：落札する、no：落札しない）、$L_{i,1}=H(b_{i,1},L_{i,2})$は入札値$b_{i,1}$のコミットメント、$\sigma_i$はコミットメント$L_{i,1}$の署名〕を受信す

る手順１と、

全入札者の入札装置からの入札が揃ったら署名σ_iが正当であることを検証し、全入札者の入札装置からの入札を公開する手順２と、

j=1とする手順３と、

入札装置からの入札値（$b_{i,j}$,$L_{i,j+1}$）を受信し、全入札者の入札値が揃ったらコミットメント$L_{i,j}$の正当性$L_{i,j}$＝H（$b_{i,j}$,$L_{i,j+1}$）を検証し、全入札値｛（$b_{i,j}$,$L_{i,j+1}$）｝を公開する手順４と、

全てのiに対して入札値$b_{i,j}$=noならj=j+1として手順４へ戻る手順５と、

あるiに対して入札値$b_{i,j}$=yesならB_iを落札者、ω_jを落札価格として決定すると共に公開する手順６とを備えたこと

を特徴とする開札方法を記録した記録媒体。

【請求項７】電子入札装置は、ネットワークを介して接続された入札装置と開札装置から構成され、

入札装置は、入札価格選択手段，入札値計算手段、コミットメント計算手段、署名計算手段及び一方向性関数記憶手段とから構成され、

入札者$B_{i(i=1,2,\cdots,n)}$は入札価格選択手段により入札価格表$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$から入札価格$\omega_{vi}$を選択し、入札値計算手段は、入札価格$\omega_{vi}$に対して入札値$b_{i,1}=b_{i,2}=\cdots=b_{i,vi-1}$=no（落札しない）、$b_{i,vi}$=yes（落札する）を計算し、コミットメント計算手段は、一方向性関数Hの連鎖を用いて入札値$b_{i,j}$に対するコミットメント$L_{i,j}$＝H（$b_{i,j}$,$L_{i,j+1}$）を計算し、署名計算手段は、コミットメント$L_{i,1}$に対しての署名σ_iを計算し、そして、入札装置は、入札（$L_{i,1}$,σ_i）を開札装置へ送信し、開札装置が署名σ_iが正当であることを検証し、全入札を公開し、さらに、入札装置は、入札値（$b_{i,j}$,$L_{i,j+1}$）を開札装置へ送信し、開札装置がコミットメント$L_{i,j}$の正当性$L_{i,j}$＝H（$b_{i,j}$,$L_{i,j+1}$）を検証し、この入札値の公開を確認したら、順次、入札値（$b_{i,j+1}$,$L_{i,j+2}$）、（$b_{i,j+2}$,$L_{i,j+3}$）、・・・を送信すると共に、

開札装置は、署名検証手段、全入札公開手段、コミットメント検証手段、全入札値公開手段、落札計算手段、落札者・落札価格公開手段及び一方向性関数記憶手段とから構成され、

署名検証手段と全入札公開手段は、入札（$L_{i,1}$,σ_i）を受信して、署名σ_iの正当性を検証すると共に、全入札を公開し、コミットメント検証手段と全入札値公開手段は、入札値（$b_{i,j}$,$L_{i,j+1}$）を受信し、コミットメント$L_{i,j}$の正当性$L_{i,j}$＝H（$b_{i,j}$,$L_{i,j+1}$）を検証すると共に、全入札値｛（$b_{i,j}$,$L_{i,j+1}$）｝を公開し、また、落札計算手段は、全てのiに対して入札値$b_{i,j}$＝noならば、j=j+1としてコミットメント検証手段、全入札値公開手段に送信し、あるiに対して入札値$b_{i,j}$＝yesならば、落札と判断して落札者・落札価格公開手段に送信し、落札者・落札価格公開手段は落札者、落札価格を公開し、

改竄などの不正がなく落札者および落札価格が正当であることを全入札者が検証可能であり、落札者以外の入札価格を秘匿し、一方向性関数の連鎖によるコミットメントを用いることにより効率的に入札を実現できること

を特徴とする電子入札装置。

【請求項８】　入札装置は、入札価格選択手段，入札値計算手段、コミットメント計算手段、署名計算手段及び一方向性関数記憶手段とから構成され、

入札者$B_{i(i=1,2,\cdots,n)}$は入札価格選択手段により入札価格表$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$から入札価格$\omega_{vi}$を選択し、入札値計算手段は、入札価格$\omega_{vi}$に対して入札値$b_{i,1}=b_{i,2}=\cdots=b_{i,vi-1}$=no（落札しない）、$b_{i,vi}$=yes（落札する）を計算し、コミットメント計算手段は、一方向性関数Hの連鎖を用いて入札値$b_{i,j}$に対するコミットメント$L_{i,j}$＝H（$b_{i,j}$,$L_{i,j+1}$）を計算し、署名計算手段は、コミットメント$L_{i,1}$に対しての署名σ_iを計算し、そして、入札装置は、入札（$L_{i,1}$,σ_i）を開札装置へ送信し、開札装置が署名σ_iが正当であることを検証し、この入札を公開し、さらに、入札装置は、入札値（$b_{i,j}$,$L_{i,j+1}$）を開札装置へ送信し、開札装置がコミットメント$L_{i,j}$の正当性$L_{i,j}$＝H（$b_{i,j}$,$L_{i,j+1}$）を検証し、この入札値の公開を確認したら、順次、入札値（$b_{i,j+1}$,$L_{i,j+2}$）、（$b_{i,j+2}$,$L_{i,j+3}$）、・・・を送信すること

を特徴とする入札装置。

【請求項９】開札装置は、署名検証手段、全入札公開手段、コミットメント検証手段、全入札値公開手段、落札計算手段、落札者・落札価格公開手段、一方向性関数記憶手段及び入札価格表$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$とから構成され、

署名検証手段と全入札公開手段は、入札者$B_{i(i=1,2,\cdots,n)}$の入札（$L_{i,1}$，σ_i）〔ただし、入札値$b_{i,1}$はω_1に対する入札値（yes：落札する、no：落札しない）、$L_{i,1}$は入札値$b_{i,1}$のコミットメント、σ_iはコミットメント$L_{i,1}$の署名〕を受信して、署名σ_iの正当性を検証すると共に、全入札｛（$L_{i,1}$，σ_i）｝を公開し、コミットメント検証手段と全入札値公開手段は、入札値（$b_{i,j}$，$L_{i,j+1}$）を受信し、コミットメント$L_{i,j}$の正当性$L_{i,j}=H$（$b_{i,j}$，$L_{i,j+1}$）を検証すると共に、全入札値｛（$b_{i,j}$，$L_{i,j+1}$）｝を公開し、また、落札計算手段は、全てのiに対して入札値$b_{i,j}$＝noならば、j=j+1としてコミットメント検証手段、全入札値公開手段に送信し、あるiに対して入札値$b_{i,j}$＝yesならば、落札と判断して落札者、落札価格公開手段に送信し、落札者・落札価格公開手段は落札者・落札価格を公開すること

を特徴とする開札装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリティ技術の応用技術に関するものであり、インターネットなどの通信ネットワーク上に分散配置された複数の入札者が、電子的な通信を利用して入札を行う、電子入札装置並びに電子入札方法及び電子入札方法を記録した記録媒体に関する。

【０００２】

【従来の技術】

従来方式の代表的な例として、宮崎、櫻井による電子入札方式(S.Miyazaki,K.Sakurai,公開掲示板を用いた秘策可能な電子入札システム、SCIS' 99 41-46 (1999))がある。

【０００３】

【発明が解決しようとする課題】

従来方式においては否認不可署名（入札者がある価格で入札していないことを証明できる署名方式）によるコミットメントが用いられていたが、否認不可署名は署名の作成／確認／否認手順に多くの計算および通信を必要とするため効率が

よくないという問題点があった。

【０００４】

【課題を解決するための手段】

本発明が提案する電子入札装置及び方法は、一方向性関数の連鎖によるコミットメントを用いて構成されているため、一方向性関数として例えばＳＨＡ－１などの実用的な一方向性関数を用いることにより、従来方式よりも効率的な入札方法を実現している。

【０００５】

【発明の実施の形態】

以下では、本発明の一実施例について説明する。

図１は、本発明の全体構成を示す図である。入札者$B_1, B_2, \cdots, B_n$(100)が開札者Ａ(200)と通信路(300)を介して結合されている。

実施例１

図２に示すように、まず開札者Ａは［前処理］を行い、次に各入札者$B_{i(i=1,\ldots,n)}$は［入札手順］(110-150)により入札を行ない、最後に開札者Ａは［開札手順］(210-250)により開札を行なう。

【０００６】

図３に入札者B_i(100)の入札手順のブロック図を示す。

図４に開札者Ａ(200)の開札手順のブロック図を示す。

［前処理］

開札者Ａは入札価格表$\{\omega_1, \cdots, \omega_{v-1}, \omega_v, \cdots, \omega_x\}$（例えば、中古車の販売で{100万円,・・・,60万円,50万円,・・・,10万円}、すなわち、開札者は価格100万円から10万円の範囲と具体的な入札価格を提示する。）および一方向性関数

$$H : \{0,1\}^s \times \{0,1\}^t \rightarrow \{0,1\}^t$$

（ただし、$\{0,1\}^s$は{0,1}の集合から成るsビットのビット列の全体集合、$\{0,1\}^t$は{0,1}の集合から成るtビットのビット列の全体集合を示す。）を決めて公開する。実際には、一方向性関数としてSHA-1などの実用的な一方向性関数を用いる。また、no（落札しないメッセージ）、yes（落札するメッセージ

) $\in \{0,1\}^s$ を公開する。

[入札手順]

入札者B_iは、図４に示す入札手順(110-150)により入札を行う。

(ステップ110)

入札者B_iは、入札価格表 $\{\omega_1, \cdots, \omega_{v-1}, \omega_v, \cdots, \omega_x\}$ から入札価格ω_{vi}を選択する（例えば、50万円）。

(ステップ120)

入札価格ω_{vi}に対する入札値

$$b_{i,j} = \begin{cases} \text{no} \in \{0,1\}^s & (1 \leqq j \leqq vi-1) \quad \text{(落札しない)} \\ \text{yes} \in \{0,1\}^s & (j = 1) \quad \text{(落札する)} \end{cases}$$

を計算する。

【０００７】

（例えば、入札者B_iは、60万円,・・・,100万円では落札を希望せず、50万円で希望する場合には、$\{\omega_1$（100万円）,・・・,ω_{v-1}（60万円）,ω_{vi}（50万円）$\}$ に対する $\{b_{i1}, \cdots b_{i,vi-1}, b_{i,vi}\}$ は {no,・・・,no,yes} となる。）

(ステップ130)

入札値$b_{i,j}$に対するコミットメント

$$L_{i,j} = H(b_{i,j}, L_{i,j+1}) \quad (1 \leqq j \leqq v_i)$$

を計算する。

【０００８】

（上記の計算は、$\{0,1\}^t$からランダムに選んだ$L_{i,vi+1}$を初期値として、$L_{i,vi} = H(b_{i,vi}, L_{i,vi+1})$,・・・,$L_{i,2} = H(b_{i,2}, L_{i,3})$,$L_{i,1} = H(b_{i,1}, L_{i,2})$ により行う。）

(ステップ140)

$b_{i,1}$に対するコミットメント$L_{i,1}$に対して、署名$\sigma_i = Sig_{Bi}(L_{i,1})$を計算する。

（この署名により入札は確かに入札者B_iが行ったものであることがわかる。）

（ステップ150）

$b_{i,1}$に対するコミットメント$L_{i,1}$とその署名σ_iの組（$L_{i,1}$、σ_i）を入札として、開札者Ａに送信する。

［開札手順］

開札者Ａは、図４に示す開札手順(210-250)により開札を行い、全入札者$B_{i(i=1,2,\cdots,n)}$に入札値｛$b_{1,1}$,$b_{1,2}$,・・・,$b_{1,vi}$｝（入札者B_1），・・・｛$b_{i,1}$,$b_{i,2}$,・・・,$b_{i,vi}$｝（入札者B_i），・・・，｛$b_{n,1}$,$b_{n,2}$,・・・,$b_{n,vi}$｝（入札者B_n）｝を順に送信させて開札手順(210-250)により開札を行う。

（ステップ２１０）

入札者B_iから入札（$L_{i,1}$,σ_i）を受信し、全入札者$B_{i(i=1,2,\cdots,n)}$からの入札｛$L_{i,1}$,σ_i｝$_{(i=1,2,\cdots,n)}$が揃ったら、署名σ_iの正当性を検証し、全入札｛($L_{i,1}$,σ_i)｝$_{(i=1,2,\cdots,n)}$を公開する。（例えば、｛（$L_{1,1}$,σ_1），・・・，（$L_{n,1}$,σ_n）｝を表示装置に表示して公開する。（この表示からは具体的な入札価格は知ることはできない。ただし、その後、入札価格等が改竄されれば｛（$L_{1,1}$,σ_1），・・・，（$L_{n,1}$,σ_n）｝が変わり、改竄されたことがわかる。）

（ステップ220）

j=1（すなわち、入札価格ω_1に対する全入札者$B_{i(i=1,2,\cdots,n)}$の入札値｛$b_{1,1}$,$b_{2,1}$,・・・,$b_{n,1}$｝、j=2（すなわち、入札価格ω_2に対する全入札者（B_1,・・・,B_i,・・・,B_n）の入札値｛$b_{1,2}$,$b_{2,2}$,・・・,$b_{n,2}$｝、・・・を順に公開すると共に、j=1,2,・・・毎に以下のステップ　(230-250)を行う。

（ステップ230）

入札者B_iから入札値（$b_{i,j}$,$L_{i,j+1}$)を受信し、全入札値｛（$b_{i,j}$,$L_{i,j+1}$)｝$_{(i=1,2,\cdots n)}$が揃ったら、コミットメントの正当性

$$L_{i,j}=H(b_{i,j},\ L_{i,j+1})$$

を検証し、全入札値｛（$b_{i,j}$、$L_{i,j+1}$）｝$_{(i=1,2,\cdots,n)}$を公開する。

（ステップ240）

全てのiに対して入札値$b_{i,j}$＝noなら、j=j+1として（ステップ230）へ戻る。

（ステップ250）

あるiに対して入札値$b_{i,j}$＝yesなら、v=jとして、B_iを落札者、ωvを落札価

格として公開する。

【０００９】

実施例２

図５は、本発明の電子入札装置のブロック図を示す。

電子入札装置１は、入札装置２と開札装置３から構成される。

入札装置１は、入札価格選択手段４，入札値計算手段５、コミットメント計算手段６、署名計算手段７及び一方向性関数記憶手段８とから構成される。

【００１０】

入札者$B_{i(i=1,2,\cdots,n)}$は、公開されている入札価格表$\omega_{j(j=1,2,\cdots,v,\cdots,x)}$９を参照して入札価格選択手段4により入札価格$\omega_{vi}$を選択する。入札値計算手段５は、入札価格$\omega_{vi}$に対する入札価格$\omega_{vi}$に対して入札値$b_{i,1}=b_{i,2}=\cdots=b_{i,vi-1}$=no（落札しない）、$b_{i,vi}$=yes（落札する）を計算する。コミットメント計算手段６は、一方向性関数Ｈの連鎖を用いて入札値$b_{i,j}$に対するコミットメント$L_{i,j}=H(b_{i,j}, L_{i,j+1})$を計算する。署名計算手段７は、コミットメント$L_{i,1}$に対しての署名$\sigma_i$を計算する。そして、入札装置２は、入札$(L_{i,1}, \sigma_i)$を開札装置へ送信し、開札装置が署名$\sigma_i$が正当であることを検証すると共に、全入札を公開し、さらに、入札装置は、入札値$(b_{i,j}, L_{i,j+1})$を開札装置へ送信し、開札装置がコミットメント$L_{i,j}$の正当性を検証し、この入札値の公開を確認したら、順次、入札値$(b_{i,j+1}, L_{i,j+2})$、$(b_{i,j+2}, L_{i,j+3})$、・・・を送信する。

【００１１】

開札装置３は、署名検証手段10-1、全入札公開手段10-2、コミットメント検証手段11-1、全入札値公開手段11-2、落札計算手段12、落札者・落札価格公開手段13及び一方向性関数記憶手段８とから構成される。

署名検証手段10-1と全入札公開手段10-2は、入札$(L_{i,1}, \sigma_i)$を受信して、署名σ_iの正当性を検証すると共に、全入札$\{(L_{i,1}, \sigma_i)\}_{(i=1,2,\cdots,n)}$を公開する。コミットメント検証手段11-1と全入札値公開手段11-2は、入札値$(b_{i,j}, L_{i,j+1})$を受信し、一方向性関数Ｈを用いてコミットメント$L_{i,j}$の正当性を検証すると共に、全入札値$\{(b_{i,j}, L_{i,j+1})\}_{(i=1,2,\cdots,n)}$を公開する。また、

落札計算手段12は、入札値$b_{i,j}$を受信し、全てのiに対して入札値$b_{i,j}$＝noならば、j=j+1としてコミットメント検証手段11-1、全入札値公開手段11-2に送信し、あるiに対して入札値$b_{i,j}$＝yesならば、落札と判断して落札者・落札価格公開手段13に送信し、落札者・落札価格を公開する。

［例外処理］

入札値（$b_{i,j}$,$L_{i,j+1}$）を公開しない入札者B_iがいる場合、その入札者B_iを除いて、再度入札をやり直す。（現実には、公開しない入札者B_iに対しては、さらに預かり金没収などの罰則を設けて対処することとなる。）

【００１２】

【発明の効果】

本発明で提案する電子入札方法および装置は、一方向性関数の連鎖によるコミットメントを用いて構成されているためSHA-1などの実用的な一方向性関数を用いることにより、否認不可署名によるコミットメントを用いていた従来方式よりも効率的な電子入札方法及び装置を実現している。

【００１３】

さらに、電子入札方法及び装置として必要な次のような性質を備えている。

［正確性］

順に入札を開示していくので、最小のvに対応するω_vで入札した入札者が落札する。

［検証可能性］

入札｛$b_{i,1}$,$b_{i,2}$,・・・,$b_{i,v}$｝とコミットメント｛$L_{i,1}$,$L_{i,2}$,・・・,$L_{i,v+1}$｝は公開されているので、だれでも改竄の検証をすることができる。

［公平性］

開札以前に公開されているのはコミットメント$L_{i,1}$のみなので、開札までは他の入札者の入札価格はわからない。

［価格秘匿性］

落札者が出たところで開札は終了し、落札者が出てきた以降の入札｛$b_{i,v+1}$,$b_{i,v+2}$,・・・,$b_{i,vi}$｝は公開されないので、落札価格以外の入札価格は秘匿されている。

［否認不可性］

コミットメント$L_{i,1}$には入札者の署名$\sigma_i = Sig_{Bi}(L_{i,1})$が付いているので否認できない。

［不正者特定可能性］

コミットメント$L_{i,j}$が公開されているので入札$b_{i,j}$を偽った者は特定できる。また、一方向性関数Hの一方向性により、コミットメント$L_{i,j}$を後から改竄することはできない。

【図面の簡単な説明】

【図１】

本発明の全体構成を示す図。

【図２】

本発明の全体的な手順を示す図。

【図３】

入札者B_iの入札手順のブロック図。

【図４】

開札者Ａの開札手順を示すブロック図。

【図５】

本発明の電子入札装置のブロック図。

【符号の説明】

1　電子入札装置

2　入札装置

3　開札装置

4　入札価格選択手段

5　入札値計算手段

6　コミットメント計算手段

7　署名計算手段

8　一方向性関数記憶手段

9　入札価格表

10-1　署名検証手段

10-2　全入札公開手段

11-1　コミットメント検証手段

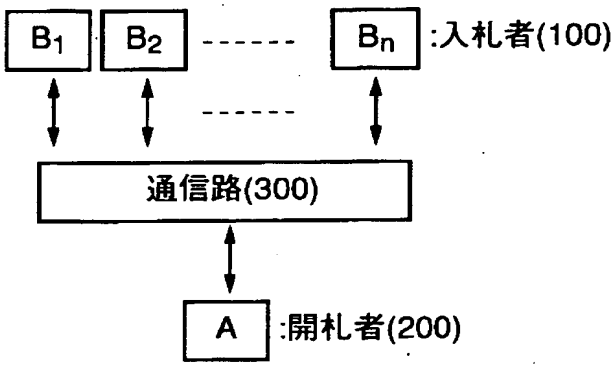
11-2　全入札値公開手段

12　落札計算手段

13　落札者・落札価格公開手段

【書類名】　図面

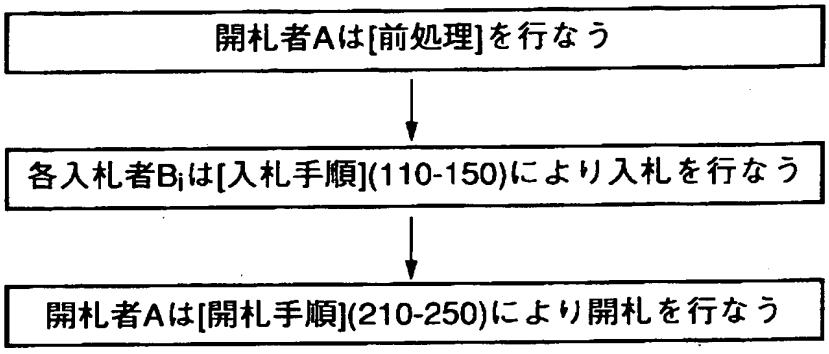
【図１】



本発明の全体構成

図　1

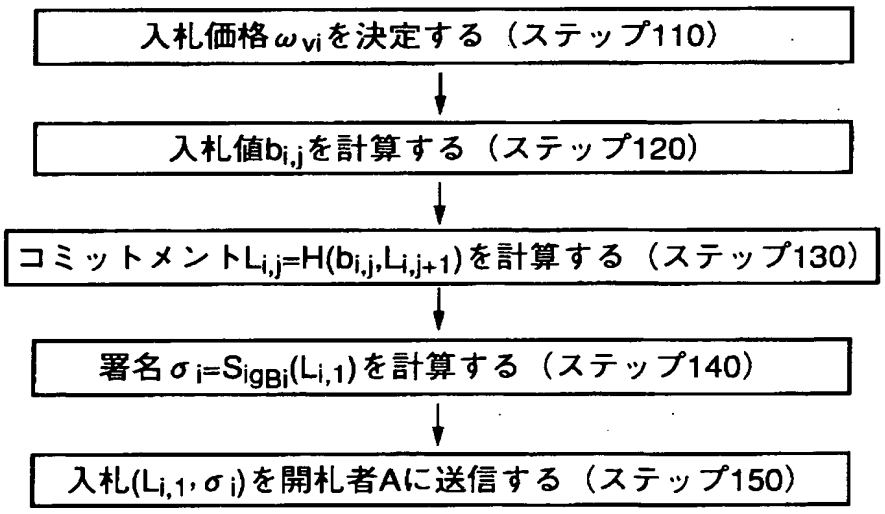
【図２】



本発明の全体的な手順

図　2

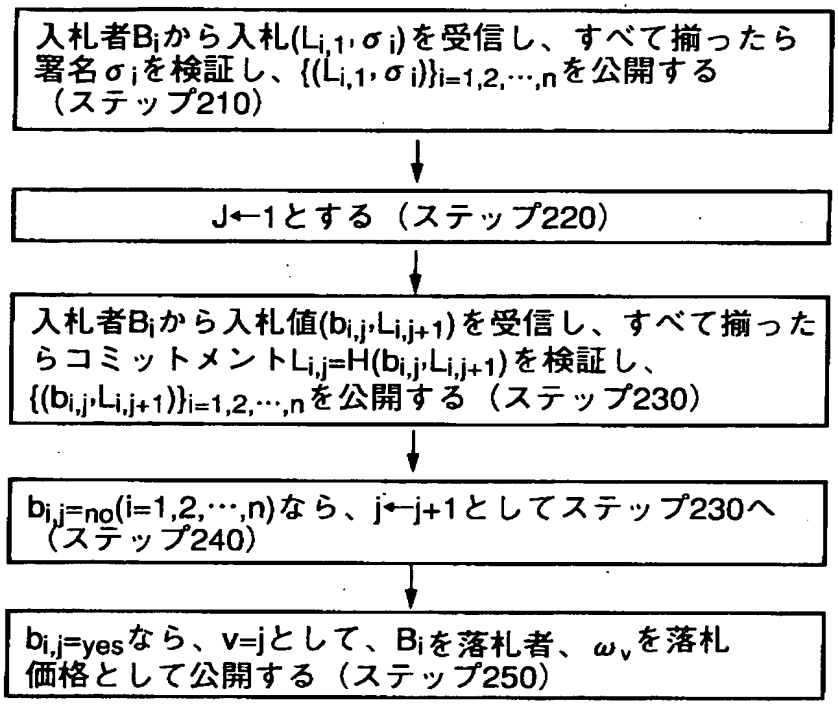
【図３】



入札者Bi(100)の入札手順のブロック図

図　3

【図４】



開札者A(200)の開札手順のブロック図

図　4

【図５】

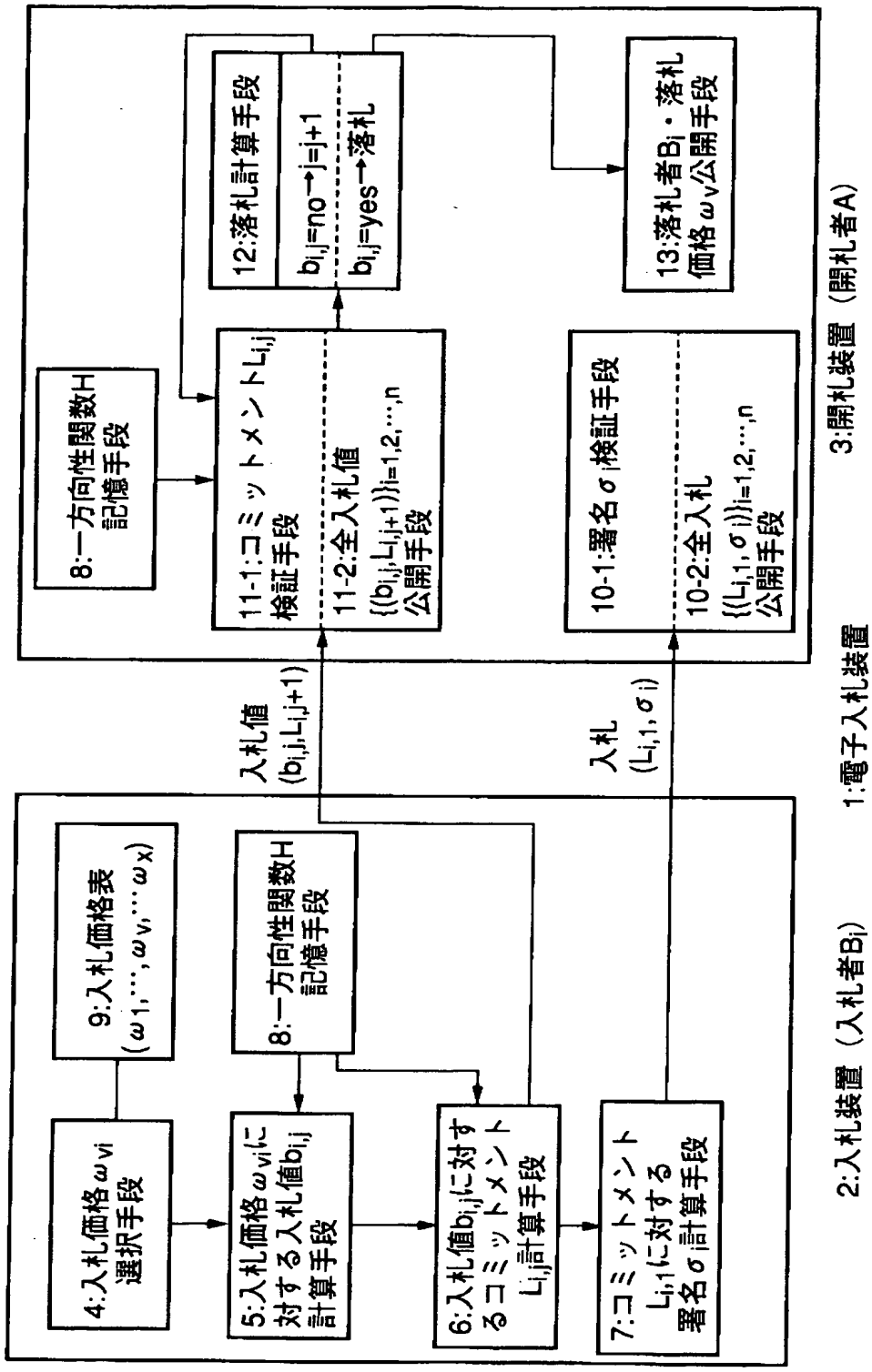

1:電子入札装置
2:入札装置（入札者Bi）
3:開札装置（開札者A）
8:一方向性関数H記憶手段
11-1:コミットメントLi,j検証手段
11-2:全入札値{(bi,j,Li,j+1)}i=1,2,…,n公開手段
12:落札計算手段
bi,j=no→j=j+1
bi,j=yes→落札
13:落札者Bi・落札価格ωv公開手段
10-1:署名σi検証手段
10-2:全入札{(Li,1,σi)}i=1,2,…,n公開手段
入札値(bi,j,Li,j+1)
入札(Li,1,σi)
9:入札価格表(ω1,…,ωv,…ωx)
8:一方向性関数H記憶手段
4:入札価格ωvi選択手段
5:入札価格ωviに対する入札値bi,j計算手段
6:入札値bi,jに対するコミットメントLi,j計算手段
7:コミットメントLi,1に対する署名σi計算手段

図 5

【書類名】　要約書

【要約】

【課題】否認不可署名によるコミットメントを用いることなく、改竄などの不正がなく落札者および落札価格が正当であることを全入札者が検証可能であり、落札者以外の入札価格を秘匿することができる電子入札方法を提供する。

【解決手段】入札装置は入札者の入札価格に対して入札値を計算し、さらに入札値に対して一方向性関数の連鎖によるコミットメントを計算し、コミットメントとその署名の組を入札として開札装置に送信すると共に、開札装置は入札を受信し、全入札者の入札が揃ったら署名が正当であることを検証し、全入札者の入札を公開し、入札装置からの入札値を受信し、全入札者の入札値が揃ったらコミットメントの正当性を検証し全入札値を公開すると共に、落札者と落札価格を決定し、公開する。

【選択図】図５

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
　［変更理由］　　住所変更
　　住　所　　東京都千代田区大手町二丁目３番１号
　　氏　名　　日本電信電話株式会社